ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

National Supervisory Control and Data Acquisition (SCADA) Test Bed

Benefits

- Apply current technologies for mitigating existing vulnerabilities.
- Establish fully functional and diverse alliances with energy, standards, and vendor communities.
- Contribute to security guidelines based on emerging threats.
- Train industry to perform self-assessments of systems to improve security.
- Provide a focal point for energy sector protection activities in vulnerability reduction and system reliability.
- Design and develop future architectures and technologies that increase system robustness against attack and enable self-healing of the infrastructures.

Applications

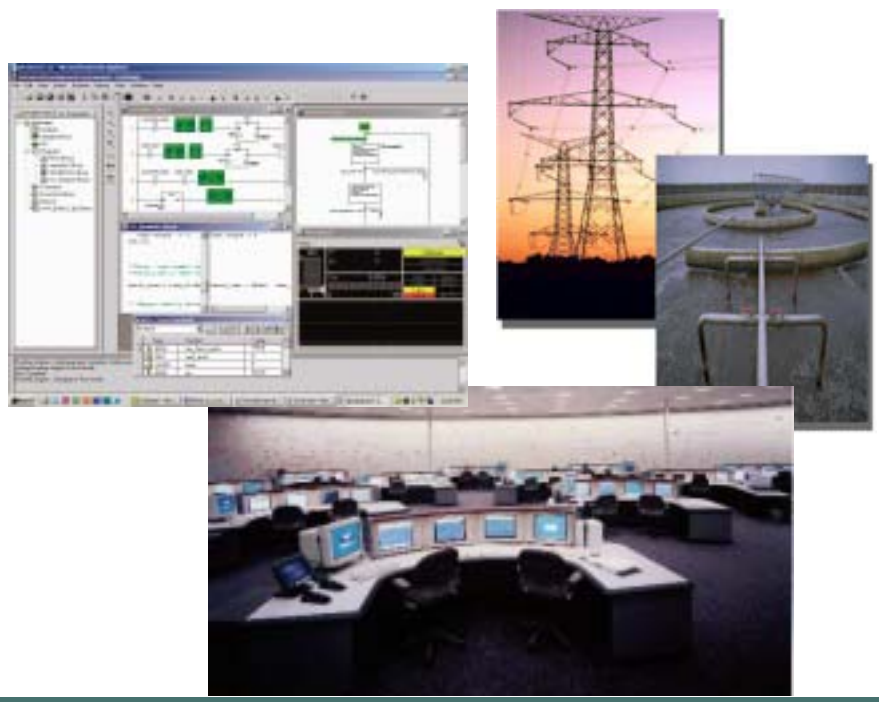
The NSTB will provide capabilities to address the utility industry's SCADA vulnerability concerns including automation and networking equipment found throughout the utility.

INCREASING ENERGY RELIABILITY BY IMPROVING THE SECURITY OF SCADA SYSTEMS

While U.S. energy systems are considered the most robust and reliable in the world, their vulnerability has now been recognized. As these systems have become increasingly dependent on powerful, electronic communications tools, the Internet, and supervisory control and data acquisition (SCADA) systems, cyber attacks have become an increasing threat.

SCADA systems are computer-based systems that monitor and control remote devices that manage commodity flows within the power grid and pipelines. Historically, SCADA systems were designed for reliability and operability, with little emphasis on security. These systems have evolved from isolated centrally controlled mainframe-based architectures using proprietary communication paths, to modern distributed networks with more potential for public access using Internet technology and common operating systems. These trends have been accelerated by deregulation, and use of common standards and interconnections between utilities.

The DOE Office of Energy Assurance (OEA) has launched a multi-laboratory partnership to implement the National SCADA Test Bed (NSTB) to test control system vulnerabilities and security hardware and software. *The National Strategy to Secure Cyberspace* calls on DOE, in cooperation with the Department of Homeland Security, other federal agencies, and the private sector, to develop best practices and new technology to increase security of distributed control and SCADA systems. The NSTB will identify SCADA vulnerabilities and recommend security standards to protect critical energy infrastructure SCADA systems. By teaming with industry, the NSTB will become a full-scale infrastructure suite of facilities for testing and validating industry control systems. Jointly run by Sandia National Laboratories and the Idaho National Engineering and Environmental Laboratory, the NSTB will integrate the critical infrastructure protection strengths of several other DOE National Laboratories including Argonne National Laboratory (oil and gas infrastructure) and Pacific Northwest National Laboratory (electricity infrastructure).



Project Partners

Sandia National Laboratories

Idaho National Engineering and Environmental Laboratory

Argonne National Laboratory

Pacific Northwest National Laboratory

U.S. Department of Energy

Interested in Participation or Additional Information About the National SCADA Test Bed, Contact:

Juan Torres
SCADA Program Manager
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185
Phone: 505-845-9804
E-mail: jjtorre@sandia.gov

Julio Rodriguez
Manager, Critical Infrastructure Assurance
Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3840
Phone: 208-526-2039
E-mail: ju2@inel.gov

For Program Information, Contact:

Hank Kenchington
Technology Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave., SW
Washington D.C. 20585
Phone: 202-586-1878
Email:
henry.kenchington@hq.doe.gov

Project Description

The NSTB provides a national program to secure the energy SCADA communications and control infrastructure. The program includes six mission areas to provide capability that will evolve from developing attack detection and prevention technologies for existing SCADA systems into a national effort to improve the security of the next-generation architectures and technology advances. The six areas of focus are as follows:

- Demonstrate energy sector vulnerabilities to industry through testing and demonstration of credible threats to the private sector, to raise awareness and develop industry acceptance of the need for improved levels of security, both physical and cyber.
- Conduct vulnerability assessments of SCADA systems to raise the awareness of equipment suppliers and utilities, and collaborate to provide near-term solutions and long-term best practice solutions into the program.
- Address disruptions in electricity, oil and gas services, and interdependent infrastructures that may require immediate and long-term remedial actions by the government and energy industries.
- Develop, with industry, technologies that provide electricity, oil and gas systems, and infrastructures that are inherently secure and dependable for their users.
- Develop risk mitigation strategies for current SCADA systems, and develop next-generation architectures for intelligent, secure infrastructures.
- Support the development of national standards and guidelines for secure SCADA design and implementation, and help align international interests with national needs by participating in development of requirements and standards.

Through laboratory partnering, the NSTB brings unique and extensive capabilities that can be leveraged to support the DOE energy assurance mission. The NSTB provides personnel with comprehensive SCADA system technical expertise and industry relationships; availability of SCADA systems, facilities, and infrastructure assets that represent real-world systems' network resources and connectivity; red teaming and assessment expertise; modeling and simulation resources; cryptography and information security capability; research and standards development support; and other SCADA-related test bed and security programs.

Progress and Milestones

- Establish a business portal for doing business with industry and government agencies. (4Q/04)
- Develop an industry liaison group charter. (4Q/04)
- Assess industry training needs related to SCADA security. (4Q/04)
- Identify applicable standards and regulatory bodies. (4Q/04)
- Issue test reports on SCADA system testing. (1Q/05)
- Establish National SCADA Test Bed VPN Network between SNL and INEEL. (4Q/04)

Economics and Commercial Potential

A disruption in the energy infrastructure can impact the security of the nation and the well-being of our citizens. Improvements in the robustness of the energy infrastructure can substantially mitigate such losses as well as address emerging cyber treats. The government, private sector (e.g., energy utilities), and general public demand a more robust and secure energy infrastructure. Such demands will, by necessity, provide significant economic and commercial opportunities.